REMARKS

By this Amendment, claims 1 and 18 are amended. Claims 2-17 and 19-22 remain in the application. Thus, claims 1-22 are active in the application. Reexamination and reconsideration of the application are respectfully requested.

On page 4 of the Office Action, claims 1-22 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicants regard as the invention. In particular, the Examiner asserted that claims 1-22 are incomplete for omitting essential structural cooperative relationships of elements because it is unclear how the encryption processing and the authentication processing can occur both in parallel and sequentially (the authentication processing is performed after the encryption processing).

Independent claims 1 and 18 have each been amended in order to clarify how the security communication packet processing apparatus and method of the present invention perform encryption processing and authentication processing in parallel and sequentially. In particular, claims 1 and 18 have each been amended to more clearly describe how the so-called pipeline structure realizes both "parallel" and "sequential" processing.

The encryption processing unit and the authentication processing unit of the security communication packet processing apparatus and the encrypting and authenticating operations of the security packet processing method of the present invention operate in parallel, but they do not perform the encryption processing and authentication processing in parallel to the same data block.

The present invention provides that the data block which is being processed by the authentication processing unit is a data block which has already been encrypted by the encryption processing unit, accumulated in the data block accumulation unit and then outputted.

Therefore, as for one data block, the authentication processing of that data block is performed **after** the encryption processing of the data block.

The encryption processing unit and the authentication unit, as well as the encrypting and authenticating operations of the method, thus operate in parallel, although they perform their respective processing to different data blocks. The security communication packet processing apparatus of claim 1 and the security communication

packet processing method of claim 18 have each been amended to clarify this feature of the present invention.

In particular, claim 1 has been amended to recite that when the inputted packet is a packet which requires both encryption processing and authentication processing, the encryption processing of a first data block by the at least one encryption processing unit and the authentication processing of a second data block by the at least one authentication unit are performed in parallel. Furthermore, clam 1 has been amended to define that the second data block to which the authentication processing is being performed is a data block which is different from the first data block and to which the encryption processing has already been performed by the at least one encryption unit and accumulated in the at least one data block accumulation unit. Claim 18 has been amended similar to claim 1.

Accordingly, the Applicants respectfully submit that claims 1 and 18 clearly and particularly define how the encryption processing and the authentication processing can occur both in parallel and sequentially. Therefore, the Applicants respectfully request withdrawal of the rejection of claims 1-22 under 35 U.S.C. § 112, second paragraph.

On page 3 of the Office Action, the Examiner reiterated the rejection of claims 1-2, 5-6, 9, 13 and 17-20 under 35 U.S.C. § 102(e) as being anticipated by Mathews (U.S. Patent Application Publication No. 2002/0078342). This rejection is respectfully traversed for the following reasons.

The present invention provides a security communication packet processing apparatus and method that, relative to conventional systems, makes it possible to speed up processing, reduce delay of the processing, increase throughput for a packet which requires authentication processing after encryption processing (although the authentication value does not need to be encrypted).

In the following description of the present invention, specific numerical values are used to aid the Examiner in understanding the invention and the marked differences between the present invention and the applied references. However, the specific numerical values used herein are merely examples, and the present invention is not to be interpreted as being limited thereto.

As mentioned above, a significant feature of the present invention is the processing of a packet which requires authentication processing after encryption

processing. In conventional systems, pipeline processing is performed per packet, i.e., packet by packet. Therefore, a buffer of a maximum packet size of 1,500 bytes, for example, is necessary for storing data which requires authentication processing after encryption processing.

However, according to the present invention, a data size which is required for authentication processing, such as 64 bytes, is an integral multiple of a data size which is required for encryption processing, such as 8 bytes, and is significantly smaller than the maximum packet size (1,500 bytes). Therefore, pipeline processing per data block of the present invention, instead of the conventional pipeline processing per packet, allows for a reduction of the buffer size to only 64 bytes for storing data which requires authentication processing after encryption processing.

Therefore, according to the present invention, it is possible to achieve a high-speed pipeline processing for encryption processing and authentication processing with a buffer size of only $1/25^{th}$ of the conventional buffer size.

The data path diagram 111 of Figure 3 illustrates the processing procedure of data blocks of a packet which requires authentication processing after encryption processing. As described beginning at line 31 on page 17 of the original specification (beginning at line 25 on page 18 of the substitute specification), a packet that requires both encryption processing and authentication processing is inputted to the a security communication packet processing apparatus and is received by an encryption processing and authentication processing control unit (referred to as "control unit" in the claims). The control unit divides the packet into data blocks for the encryption processing, and sequentially transmits the data blocks along with processing information thereof to an encryption processing unit. The encryption processing unit encrypts the data blocks according to an appropriate processing method based on the processing information.

The encrypted data blocks are outputted to a packet construction unit, and at the same time, are outputted to a data block accumulation unit. The data block accumulation unit successively accumulates the encrypted data blocks outputted form the encryption processing unit until the accumulated encrypted data blocks reach the data block size that is necessary for the authentication processing. Accordingly, the data block accumulation unit acts as a buffer by accumulating the encrypted data blocks until the amount of the

accumulated data blocks reaches the data block size that is necessary for the subsequent authentication processing. When the accumulated encrypted data blocks reach the data block size (e.g. 64 bytes) that is necessary for the authentication processing, the data block accumulation unit outputs the accumulated data blocks and the processing information thereof to an authentication processing unit.

The authentication processing unit receives the accumulated encrypted data blocks and the processing information thereof, performs authentication processing on the encrypted data blocks according to the processing information, and calculates an authentication value. The authentication processing unit then outputs the authentication value to a packet construction unit, which has already received the encrypted data blocks outputted from the encryption processing unit.

The packet construction unit then constructs (reconstructs) an encrypted and authentication-processed packet corresponding to one packet that is inputted to the control unit by accumulating the encrypted data blocks outputted from the encryption processing unit, and incorporating the authentication value outputted from the authentication processing unit. See data path diagram 111 of Figure 3 for a pictorial explanation of the above-described operation.

Accordingly, for a packet that requires both encryption processing and authentication processing, the present invention provides that the authentication value does not need to be encrypted, whereas, as described further below, Mathews performs parallel processing of a packet of plain text which requires encryption processing and authentication processing, where the authentication value needs to be encrypted.

Furthermore, the present invention includes a data block accumulating unit (i.e., a buffer) between the encryption processing unit and the authentication processing unit. The size which is required for this buffer can be reduced to the data block size that is necessary for performing the authentication processing.

Independent claims 1 and 18 each recite these novel features of the present invention. In particular, claim 1 recites the security communication packet processing apparatus as comprising at least one encryption processing unit operable to perform the encryption processing and the decryption processing in a data block unit of B1 bits. Further, claim 1 recites the security communication packet processing apparatus as

comprising at least one data block accumulation unit operable to accumulate the data blocks to which the encryption processing **has been performed** by the at least one encryption processing unit, and, when the amount of accumulated data blocks reaches B2 bits (B2 = n x B1), output the data blocks to at least one authentication processing unit. The security communication packet processing apparatus of claim 1 is also recited as comprising the at least one authentication processing unit operable to perform the authentication processing in a data block unit of B2 bits in parallel to the encryption processing or the decryption processing performed by the at least one encryption processing unit, and output an authentication value indicating the result of the authentication processing, the data block unit of B2 bits being n times the data block unit of B1 bits.

The security communication packet processing method of claim 18 is recited as comprising performing the encryption processing or the decryption processing to the divided data blocks of B1 bits, and accumulating the encrypted data blocks and outputting the data blocks when the amount of accumulated data blocks reaches B2 bits (B2 = n x B1). The security communication packet processing method of claim 18 is also recited as performing the authentication processing to the outputted data blocks (encrypted data blocks) of B2 bits in parallel to the encryption processing or the decryption processing, and outputting the authentication value indicating the result of the authentication processing.

Mathews discloses a cryptography accelerator chip that performs parallel processing of a packet of plain text which requires encryption processing and authentication processing, where the authentication value needs to be encrypted. In particular, Mathews discloses that the chip architecture includes an authentication component 302 and an encryption (or decryption) component 352. The authentication component 302 includes an authentication alignment block 304 which removes non-valid bytes of a packet and packs and aligns data to be input into an authentication FIFO buffer 306 (see paragraph [0027]). Once 512 bits or a complete packet worth of data padded to a multiple of 512 bits have been loaded into the authentication FIFO buffer 306, Mathews discloses that the authentication value is then fed back into the encryption component 352. Specifically, the encryption alignment block 354 receives data for cryptography

processing from a front end source 301 and the feedback of the authentication value outputted from the authentication engine 308 (see arrow 309 of Figure 3 and paragraphs [0028]-[0029]).

Accordingly, for processing a packet or stream of data that requires both encryption processing and authentication processing, Mathews discloses that the authentication value must then be encrypted by the encryption alignment block 354. Furthermore, Mathews includes respective buffers in the stages prior to the authentication processing (FIFO 306) and the encryption processing (FIFO 356). In particular, Mathews requires a buffer of an authentication value size (512 bits) or larger (that is, larger than the encryption block size) in the stage prior to the encryption processing.

In stark contrast to Mathews, claim 1 recites the security communication packet processing apparatus as comprising at least one data block accumulation unit operable to accumulate the data blocks to which the encryption processing **has been performed** by the at least one encryption processing unit, and, when the amount of accumulated data blocks reaches B2 bits (i.e., an integral multiple of a unit of data on which encryption processing has been performed), output the data blocks to at least one authentication processing unit. In addition, the security communication packet processing method of claim 18 is recited as comprising performing the encryption processing or the decryption processing to the divided data blocks of B1 bits, and accumulating the encrypted data blocks and outputting the data blocks when the amount of accumulated data blocks reaches B2 bits.

Therefore, in view of the above, Mathews clearly does not disclose or suggest each and every limitation, as Mathews discloses that for a packet or stream of data requiring encryption processing and authentication processing, the authentication value must be encrypted, and Mathews requires an authentication buffer (FIFO 306) to be larger than an encryption block data size.

Furthermore, Mathews discloses a parallel processing method with regard to a packet or stream of data that requires both encryption processing and authentication processing, whereas the present invention employs a pipeline data processing method for a packet that requires both encryption processing and authentication processing. In addition, the apparatus and method of the present invention are different in effect to the

chip structure of Mathews, because the present invention provides a reduction of a buffer size in the processing in addition to high-speed processing, whereas Mathews merely provides high-speed processing.

Accordingly, in view of the above, Mathews clearly does not disclose or a suggest a security communication packet processing apparatus as comprising at least one data block accumulation unit operable to accumulate the data blocks to which the encryption processing has been performed by the at least one encryption processing unit, and, when the amount of accumulated data blocks reaches B2 bits (i.e., an integral multiple of a unit of data on which encryption processing has been performed), output the data blocks to at least one authentication processing unit, as recited in claim 1. Similarly, Mathews clearly does not disclose or suggest a security communication packet processing method of claim 18 is recited as comprising performing the encryption processing or the decryption processing to the divided data blocks of B1 bits, and accumulating the encrypted data blocks and outputting the data blocks when the amount of accumulated data blocks reaches B2 bits, as recited in claim 18.

Therefore, claims 1 and 18 are clearly not anticipated by Mathews since Mathews fails to disclose or suggest each and every limitation of claims 1 and 18.

In rejecting claim 2, the Applicants note that the Examiner referred to paragraph [0031] in alleging that Mathews discloses the processing performed for a packet of the first type which requires both encryption and authentication processing. However, paragraph [0031] of Mathews discloses the decryption process performed by Mathews, where decrypted data is fed back to the authentication alignment block 304 of the authentication component 302.

Dependent claim 20 recites that the data block accumulation unit may be bypassed. Specifically, claim 20 recites that some of the data blocks (A) pass through the data block accumulation unit and other data blocks (B) bypass the data block accumulation unit (buffer) depending on the data block type. Thus, as recited in claim 20, the present invention provides that data blocks which do not need to be accumulated by the data block accumulation unit bypass the data block accumulation unit, which results in high-speed processing.

However, in Mathews, FIFO 306 (and FIFO 356) are always connected

immediately previous to the authentication engine 308 (and the cryptography engine 358 (see paragraph [0024] and the authentication alignment 304 and the cryptography alignment 354 in Figure 3). In other words, all the data blocks pass through the buffer in Mathews. Accordingly, Mathews also fails to disclose or suggest the limitations recited in claim 20.

Dependent claim 21 recites that data blocks are saved and restored via the data block accumulation unit. Therefore, in the case where a higher priority data block is inputted during the buffering of a data block, the processing order can be optimized so that the higher priority data block is processed first. Mathews does not even contemplate this feature of the present invention. Therefore, similar to claims 1, 18 and 20, Mathews clearly does not disclose or suggest the invention of claim 21.

Dependent claim 22 recites that the suspended data block(s) can be passed on to another processing unit having an equivalent processing function. Therefore, the present invention makes it possible to reduce the number of processing units in a ready-for-processing state and thus achieve high-speed processing. Mathews also does not even contemplate this feature of the present invention.

Accordingly, at least for the foregoing reasons, Mathews clearly does not disclose or suggest each and every limitation of claims 1 and 18, as well as claims 20-22.

On page 3 of the Office Action, the Examiner reiterated the rejection of claims 3-4, 7-8, 10-12 and 14-16 under 35 U.S.C. § 103(a) as being unpatentable over Matthews in view of Videcrantz et al. (U.S. 6,275, 588).

As demonstrated above, Mathews clearly fails to disclose or suggest each and every limitation of claims 1 and 18, as well as new claims 20-22. However, Videcrantz et al. fails to cure the deficiencies of Mathews for failing to disclose or suggest each and every limitation of claims 1 and 18, as well as new claims 20-22.

Therefore, no obvious combination of Mathews and Videcrantz et al. would result in the inventions of claims 1 and 18 or any claims depending therefrom since Mathews and Videcrantz et al., either individually or in combination, fail to disclose or suggest each and every limitation of claims 1 and 18.

Furthermore, it is submitted that the clear distinctions discussed above are such that a person having ordinary skill in the art at the time the invention was made would not

have been motivated to modify Mathews and Videcrantz et al. in such as manner as to result in, or otherwise render obvious, the present invention as recited in claims 1 and 18. Therefore, it is submitted that the claims 1 and 18, as well as claims 2-17 and 19-22 which depend therefrom, are clearly allowable over the prior art as applied by the Examiner.

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. An early notice thereof is respectfully solicited.

If, after reviewing this Amendment, the Examiner feels there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

Yuusaku OHTA et al.

By: _____
Jonathan R. Bowser
Registration No. 54,574
Attorney for Applicants

JRB/nrj
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
February 23, 2006